eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Online Brute Force:**
  - ✓ Conceitos
  - ✓ Alvos
  - ✓ Ferramentas
  - ✓ Wordlist com MZTG
- ✓ **Patator**
  - ✓ Conceito
  - ✓ Exemplo

Online Brute Force

Online Brute Force: Conceito

O ataque de Brute Force na modalidade Online é o mais difícil de ser aplicado, não pelo fator técnico, mas, pela limitação de infraestrutura.

Diferente dos ataques off-line, que realizamos milhões de tentativas por segundo, na modalidade online as tentativas caem para, em média, uma por segundo, isso quando não há proteções que dificultam ainda mais esse processo.

Existem casos que pode-se apenas testar uma senha por minuto.

A explicação para isso é fácil. Quando realizamos testes online, geramos log, ou seja, nossos testes se tornam barulhentos aos firewalls, IDSs ou até mesmo ao Sistema Operacional.

Para um processo de Pentest, quanto mais sorrateiro forem os testes, melhor.

Online Brute Force: Alvos

Depois de se esgotarem as tentativas de se conseguir a senha e tentar faze-la off-line, temos então que partir para o ataque online.

Quanto lidamos com uma página web, podemos tentar conseguir a senha através de exploração de falhas. Quando não a encontramos, temos que apelar para o ataque online.

Não temos apenas servidores web para realizar os testes, temos qualquer dispositivo conectado a uma rede e que requeira de autenticação.

Em um Pentest, temos que realizar varreduras para que detectemos quem serão nossos alvos e as vezes, esses alvos não são muito claros; como por exemplo, o serviço ssh com a porta alterada.

Online Brute Force: Ferramentas

Existem diversas ferramentas que podemos utilizar para realizar os testes de senhas durante o processo de um Pentest. São elas:

- Hydra
- Medusa
- Patator
- Burpsuite
- entre outros ...

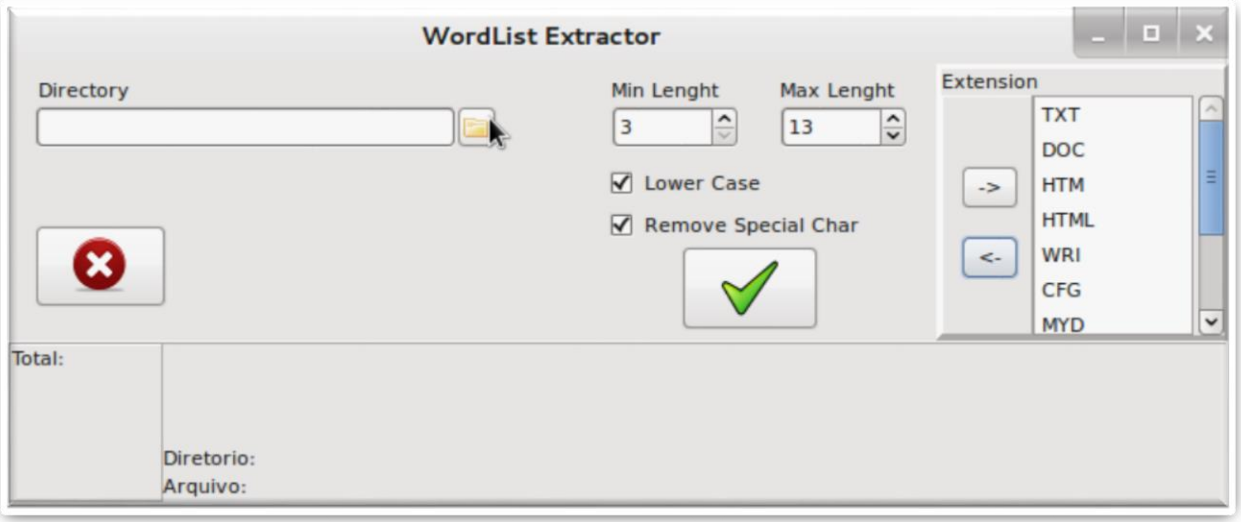
Online Brute Force: WL com MZTG

MZTG é um aplicativo multiplataforma desenvolvido para gerar wordlists de forma inteligente.

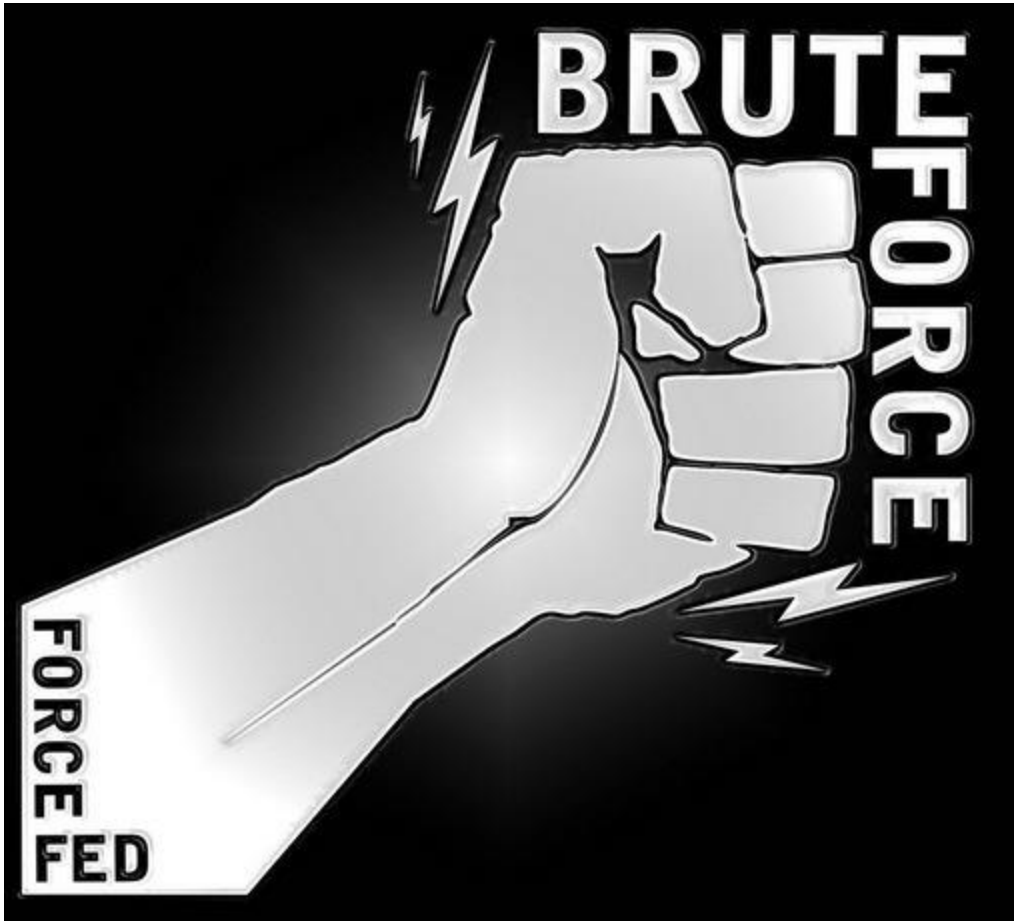
Através de combinações entre wordlists, dados previamente imputados e sequência de caracteres é possível criar wordlists mais eficazes.

As wordlists customizadas aumentam em 80% a eficaz de uma auditoria de senhas.

Você pode baixar a ferramenta no site oficial do MZTG (www.mztg.org).



Patator



Patator

Patator é uma ferramenta desenvolvida em python que tem como objetivo realizar teste de bute-force nos mais diferentes tipos de protocolos e tecnologias

Algumas Características:

- Sem falsos negativos, como é o usuário que decide o que resulta ignorar baseado em:
    - o código de estado da resposta
    - tamanho de resposta
    - string ou regex correspondência em dados de resposta
- Design modular
- Mostra o progresso detalhado
- Sistema de Pause / Resume
- Aumenta e diminui a Verbosidade
- Adiciona novas ações e condições durante o tempo de execução
- Utiliza conexões persistentes (ex. Testará várias senhas até que se desligue o servidor)
- Multi-threaded

Patator: Exemplo

A usabilidade do Patator é parecida com o Hydra e Medusa, porém, com pequenas características diferenciadas.

É possível utiliza-lo para quebra de senhas online e também off-line.

Vamos neste exemplo tentar quebrar um arquivo compactado e com senha.
patator unzip_pass zipfile=mensagem.zip password=FILE0 0=pass.txt -x ignore:code!=0

Patator – Aplicação de recuperação de senha
Unzip_pass – Módulo utilizado
Zipfile – Caminho do arquivo compactado
Password – Tipo de Autenticação
FILE0 – Arquivo 0, podem ser utilizados mais do que um arquivo, exemplo: FILE2.
0 – É o arquivo setado. No caso acima, onde podemos setar o FILE2, podemos usar a opção 0=arquivo0.txt 1=arquivo1.txt e 2=arquivo2.txt
-x – Mensagem de retorno, onde podemos filtrar o que queremos ver.

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker